BROCADE

WHITE PAPER

Brocade Virtual Web Application Firewall

Network Deployment Options

TABLE OF CONTENTS

Introduction

Brocade® Virtual Web Application Firewall (vWAF) supports a full range of deployment options enabling you to choose the best fit for your architecture and application risk profile. Brocade vWAF can be deployed as a virtual appliance, on a web server, or as a physical appliance in a customer data center or cloud provider—or even as an integrated package with Brocade Virtual Traffic Manager (vTM) for enhanced security and control of complex applications.

In addition, Brocade vWAF is also available as a stand-alone proxy, designed to be used with existing load- balancers and ADCs, and is particularly suitable for cloud deployment to add application-level security to a cloud application without changing the application architecture.

Brocade Virtual Web Application Firewall Deployment Options

A range of deployment options is available to suit any kind of IT environment:

- **Brocade vWAF add-on for Brocade vTM:** This module may be licensed for Brocade vTM (software or virtual appliance), and allows the Brocade vTM to enforce application-level security to traffic.
- **Brocade vWAF Web server plug-in:** For maximum scalability in global applications, the Brocade vWAF can be implemented as Web server plug-ins providing a fully distributed architecture with complete flexibility.
- **Brocade vWAF proxy solution:** This stand-alone Brocade vWAF proxy solution is available as either a software or virtual appliance, and is typically deployed alongside an existing ADC or load balancer device. The existing ADC routes traffic through the proxy so that the Brocade vWAF can apply deep application-level security.

Deploying Brocade vWAF Add-on for Brocade vTM

Brocade vWAF for Brocade vTM is enabled via license key as a capability of the Brocade vTM. The network deployment options are same as Brocade vTM network configurations as described in Chapter 2 of the user guide located at http://brocade.com/vadc-docs (See Figure 1).

Deploying Brocade vWAF Web-Server Plug-In

The fully distributed version of Brocade vWAF is installed as a Web server plug-in and is therefore very simple to deploy from a network perspective. For more details on installation and deployment, please refer to the support and documentation pages at http://brocade.com/vadc-docs (See Figure 2.)

Deploying Brocade vWAF Proxy Solutions

Brocade vWAF proxy solution is deployed as a stand-alone proxy device either sandwiched within an existing ADC deployment (much like a firewall or other proxy device) or in front of a single Web server. The remainder of this document discusses deployment scenarios for Brocade vWAF.

Brocade vWAF for Load-Balanced Environments

Brocade vWAF can be deployed in an existing load-balanced scenario without having to change or rewire the existing network topology. Logically, Brocade vWAF devices are sandwiched between two layers of ADCs so that they can be scaled, and the ADCs perform the health-checks and load balancing against the back-end servers.

Deployment alongside an Existing ADC or Load Balancer

Although the logical design of the software calls for a network "sandwich" between two ADC layers, in practice the deployment is generally performed with a single layer of ADCs. This ADC layer runs two load-balancing services; one to forward traffic out to the Brocade vWAF devices, and one to load-balance traffic from the devices across the backend servers. This configuration, which loops traffic out to the Brocade vWAFl devices, is sometimes referred to as a network "trombone" (See Figure 3 on the following page).

Brocade vWAF can be deployed in one of the following ways:

1. One-armed deployment (single network segment)
2. Two-armed deployment (public and private network segments)

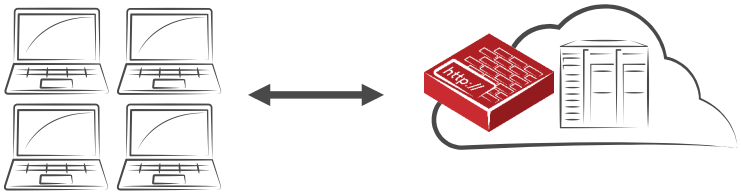

Figure 1: Brocade vWAF deployed as an add-on module for the Brocade vTM.

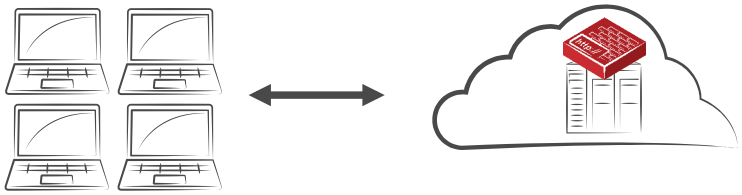

Figure 2: Brocade vWAF plug-in modules deployed on the Web server.

One-Armed Deployment

In a one-armed deployment, Brocade vWAF is deployed in the same VLAN/network as Web/application servers, and the single interface on the device connects to the internal network.

As depicted in the Figure 4, traffic flow for this deployment mode is as follows:

1. The FQDN for the application that needs to be protected resolves to an external IP address on the Traditional ADC. The client makes a TCP connection to this IP address.
2. The traditional ADC is configured to load balance HTTP traffic across one or more Brocade vWAF instances.
3. Brocade vWAF analyzes incoming traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the incoming traffic is forwarded to the application Web/applications servers. (Note: If any response needs to go back through the traditional ADC, either the ADC must also function in full-proxy mode or source-NAT needs to be configured on the ADC, or the vWAF default-gateway should be the ADC*).*
4. The Web server processes the request, and send the response to Brocade vWAF via the ADC.
5. Brocade vWAF analyzes outgoing traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the outgoing traffic is sent to the client via the ADC.

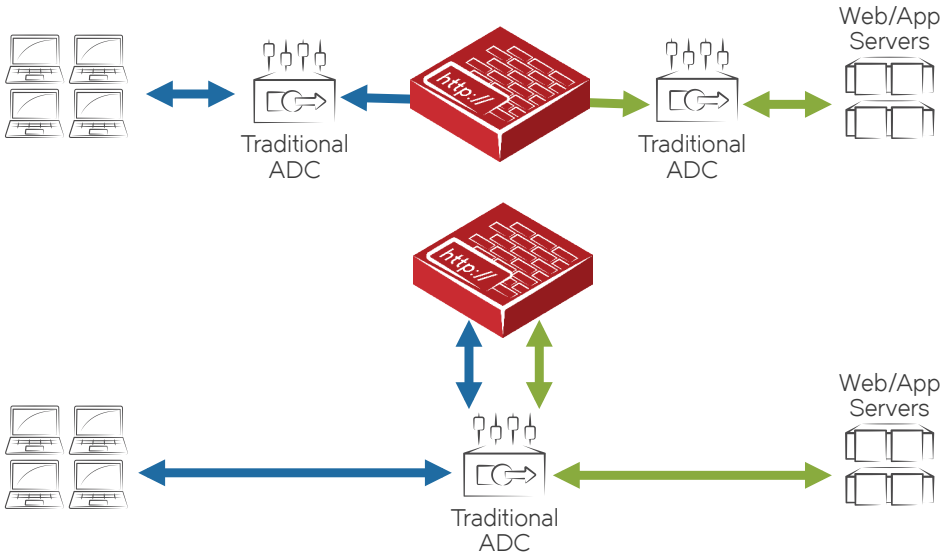

Figure 3: Logical "sandwich" view of deployment (top) and typical "trombone" deployment (bottom) that eliminates the need for two layers of ADCs.

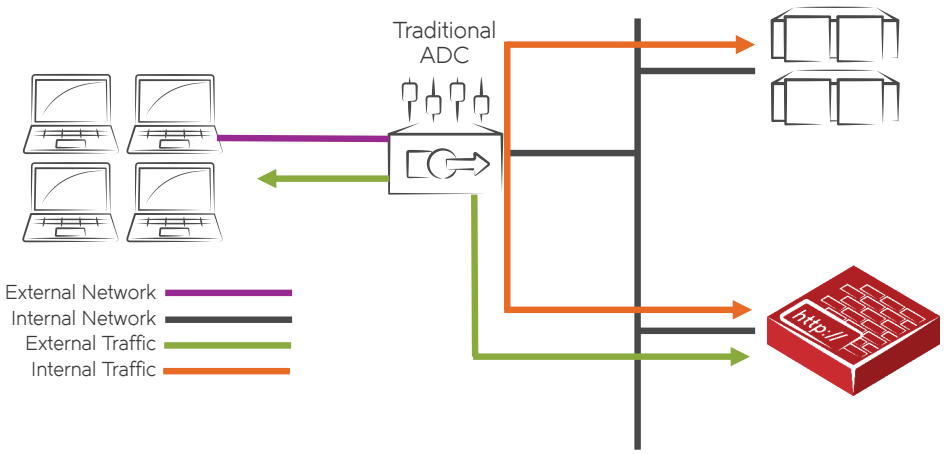

Figure 4: Deployment alongside an existing ADC or load balancer: One-armed Deployment.

Two-Armed Deployment

In this mode of deployment, Brocade vWAF is connected to the external and internal network as depicted in Figure 5.

Traffic flow for this deployment mode is as follows:

1. The FQDN for the application that needs to be protected resolves to an external IP address on the Traditional ADC. The client makes a TCP connection to this IP address.
2. The traditional ADC is configured to load balance HTTP traffic to Brocade vWAFl or across a pool of Brocade vWAF devices with external IP addresses.
3. Brocade vWAF analyzes incoming traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the incoming traffic is forwarded to the application Web/applications servers. (Note: that if any response needs to go back through the traditional ADC, either the ADC must also function in full-proxy mode or source-NAT needs to be configured on the ADC, or the Brocade vWAFdefault- gateway should be the ADC.)
4. The Web server processes the request, and sends the response to Brocade Web Application Firewall via the ADC.
5. Brocade Web Application Firewall analyzes outgoing traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the outgoing traffic is sent to the client via the ADC.

If necessary, an additional management interface can be configured on Brocade Web Application Firewall and then connected to a separate management VLAN or network.

Brocade Web Application Firewall Scalability

The ADC may load-balance traffic across multiple independent Brocade Web Application Firewall nodes. The ADC should apply session persistence so that all traffic from the same client is directed to the same Brocade Web Application Firewall instance.

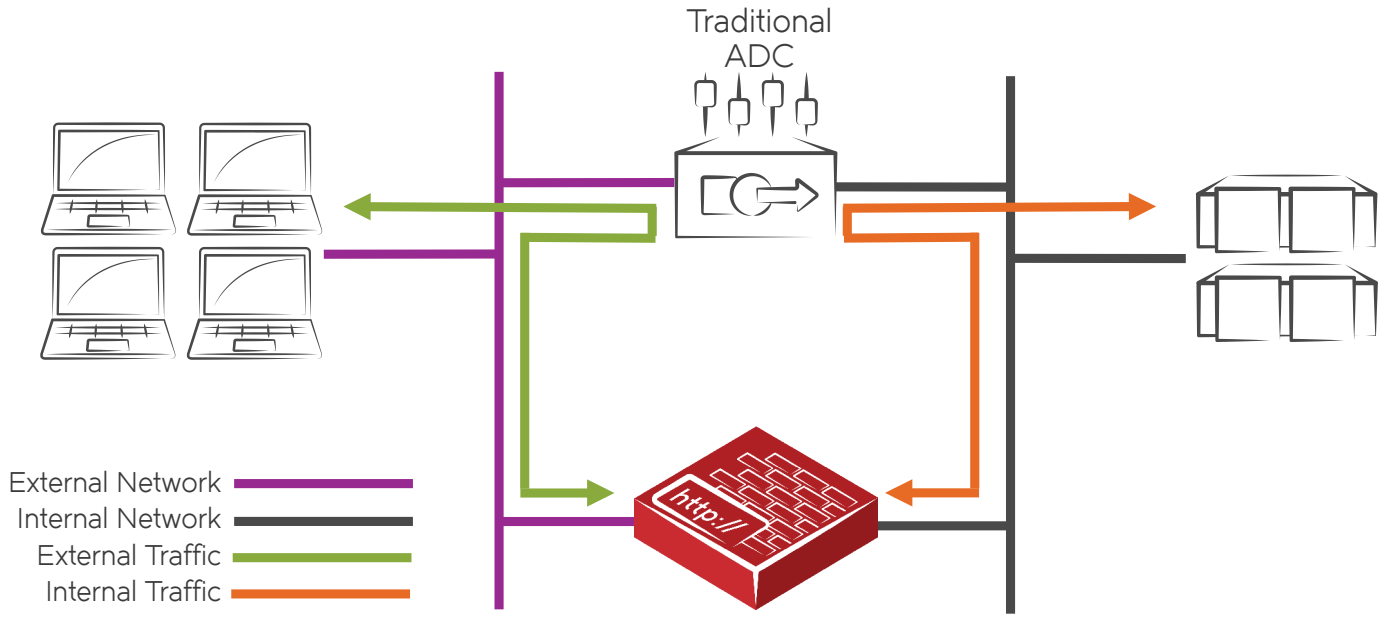

Figure 5: Deployment alongside an existing ADC or load balancer: Two-armed Deployment.

Brocade vWAF Deployed without a Local ADC or Load-Balancer

In some scenarios, a local ADC or load balancer may not be present. The Web Application may be served from a single web server, or a technique like round robin DNS may be used to distribute traffic across the servers. In this situation, Brocade vWAF is deployed as a proxy, receives external traffic, and then forwards it on to the Web servers.

Some configuration changes to the DNS need to be made in order to ensure that the traffic would be directed to Brocade vWAF. Otherwise an IP address reassignment is necessary.

Deploying Brocade vWAF with a Single Web Server

Brocade vWAF is configured as a simple proxy with a single virtual server and pool. Incoming traffic is routed to the Brocade vWAF virtual server and the pool forwards it to the back-end server. Either a one-armed or a two-armed deployment may be used (See Figure 6).

Deploying Brocade vWAF with a Group of Web Servers

In this scenario, a load balancer or an ADC is needed to forward traffic to a group of Web servers. However, in limited cases, a load balancer or DNS round robin solution may be in use. But without administration privileges or if the load balancer is not local, it may not be possible to use the configuration described in the previous section. In such cases, the stand-alone device can be deployed with multiple virtual server and pool pairs, one for each back-end Web server (See Figure 7).

Once again, either a one-armed or two-armed deployment model may be used.

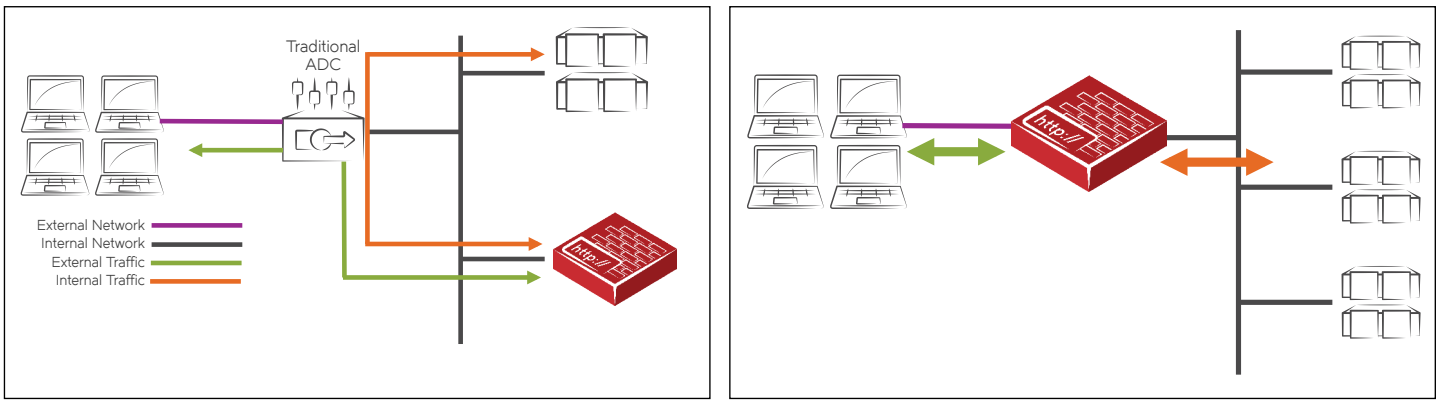

Figure 6: Deploying Brocade vWAF with a single Web server.

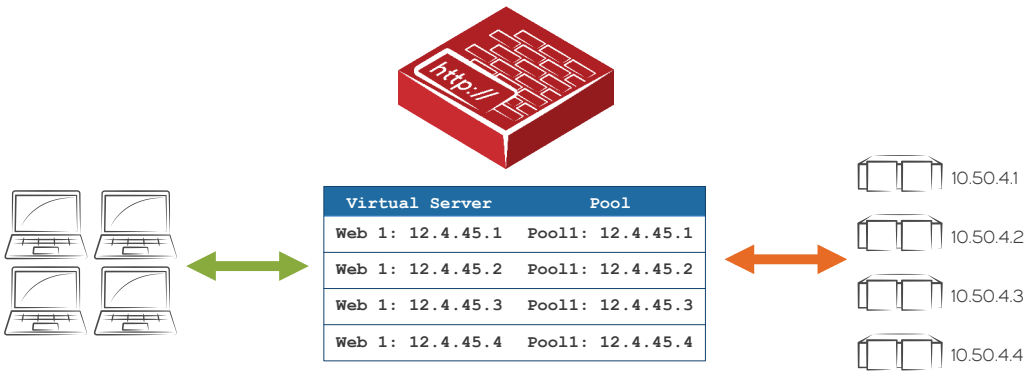

Figure 7: Deploying Brocade vWAF with a group of Web servers.

Brocade vWAF Scalability

Brocade vWAF may be deployed in a fault-tolerant cluster consisting of two or more devices. Brocade vWAF clusters manage a floating set of IP addresses (called "Traffic IPs") and ensure that the cluster manages traffic directed to those IP addresses, even in the event of a Brocade vWAF failure. For high scalability needs, the cluster may be run in an Active/Active fashion, allowing for linear scalability of capacity.

Conclusion

The range of Brocade Web Application Firewall platforms and deployment options make it possible to apply vWAF optimizations to almost any Web-based application:

- Brocade vWAF add-on for Brocade vTM may be added to an existing Brocade vTM ADC
- Brocade vWAF web-server plug-ins may be deployed for maximum scalability in global applications
- Brocade vWAF proxy solutions may be deployed to augment an existing load-balanced or single-server environment

Brocade vWAF platforms support multiple network topologies and can be provisioned as both software and a packaged virtual appliance, making it easy to accelerate existing enterprise or online applications and free development teams from the burden of content optimization and testing.

About Brocade

Brocade networking solutions help organizations achieve their critical business initiatives as they transition to a world where applications and information reside anywhere. Today, Brocade is extending its proven data center expertise across the entire network with open, virtual, and efficient solutions built for consolidation, virtualization, and cloud computing. Learn more at www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE